Dr. James Mickens
Direct Examination

Summary of Conclusions

iPhone's security guarantees are predominantly enforced by the iPhone's operating system (iOS)

Evidence suggests that the App Review process does a weak job of enforcing additional security properties that cannot be enforced by the OS alone

iOS, much like macOS, is already capable of installing applications that were not distributed via Apple's App Store

If Apple allowed iPhone users to opt into third-party app distribution channels, those users would not suffer from a meaningfully less-secure experience

Mickens Direct Written Testimony ("DWT") Section II

How is Security Enforced on iPhones?

OFF-DEVICE SECURITY
app distribution

Can be performed by third parties

- App Review
- Developer Identification
- Code Signing

Provides minimal (if any) security benefits relative to what iOS on-device security mechanisms provide

ON-DEVICE SECURITY
operating system

Independent of app distribution method

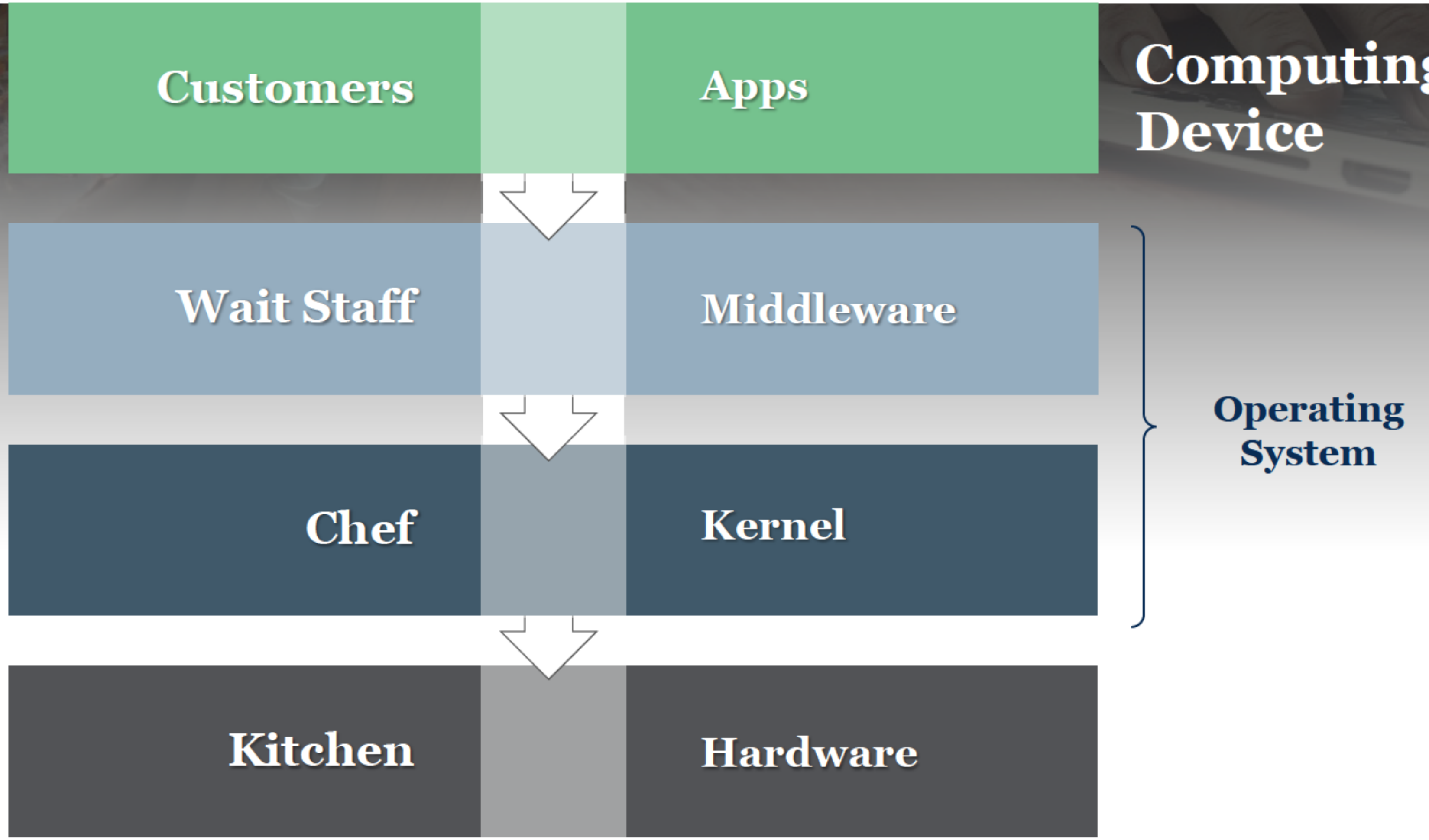
- Digital Signature Validation
- Sandboxing
- Address Space Layout Randomization (ASLR)
- Execute Never (W^X)
- Memory Isolation
- Kernel Integrity Protection
- Page Protection Layer

ON-DEVICE SECURITY
hardware

- Biometric Authentication
- Secure Enclave
- Storage Encryption
- Secure Boot

Mickens DWT ¶6, Sections V, VII

Operating System Design



Restaurant	Computing Device
Customers	Apps
Wait Staff	Middleware
Chef	Kernel
Kitchen	Hardware

Operating System

On-Device Security: Operating System

OFF-DEVICE SECURITY
app distribution

app

Can be performed by third parties

- App Review
- Developer Identification
- Code Signing

Provides minimal (if any) security benefits relative to what iOS on-device security mechanisms provide

ON-DEVICE SECURITY
operating system

iOS

- Digital Signature Validation
- Sandboxing
- Address Space Layout Randomization (ASLR)
- Execute Never (W^X)
- Memory Isolation
- **Kernel Integrity Protection**
- **Page Protection Layer**

Memory protection for the kernel

ON-DEVICE SECURITY
hardware

- Biometric Authentication
- Secure Enclave
- Storage Encryption
- Secure Boot

On-Device Security: Operating System

OFF-DEVICE SECURITY
app distribution

Can be performed by third parties

ON-DEVICE SECURITY
operating system

ON-DEVICE SECURITY
hardware

- App Review
- Developer Identification
- Code Signing
- Digital Signature Validation
- Sandboxing
- **Address Space Layout Randomization (ASLR)**
- **Execute Never (W^X)**
- **Memory Isolation**
- Kernel Integrity Protection
- Page Protection Layer
- Biometric Authentication
- Secure Enclave
- Storage Encryption
- Secure Boot

Provides minimal (if any) security benefits relative to what iOS on-device security mechanisms provide

Memory protection for both the kernel and apps

On-Device Security: Operating System

OFF-DEVICE SECURITY
app distribution

app

Can be performed by third parties

- App Review
- Developer Identification
- Code Signing

Provides minimal (if any) security benefits relative to what iOS on-device security mechanisms provide

ON-DEVICE SECURITY
operating system

iOS

- Digital Signature Validation
- **Sandboxing**
- Address Space Layout Randomization (ASLR)
- Execute Never (W^X)
- Memory Isolation
- Kernel Integrity Protection
- Page Protection Layer

Isolates misbehaving processes

ON-DEVICE SECURITY
hardware

- Biometric Authentication
- Secure Enclave
- Storage Encryption
- Secure Boot

Mickens DWT Sections V, VII

On-Device Security: Operating System

OFF-DEVICE SECURITY
app distribution

app

Can be performed by third parties

- App Review
- Developer Identification
- Code Signing

Provides minimal (if any) security benefits relative to what iOS on-device security mechanisms provide

ON-DEVICE SECURITY
operating system

iOS

- **Digital Signature Validation**
- Sandboxing
- Address Space Layout Randomization (ASLR)
- Execute Never (W^X)
- Memory Isolation
- Kernel Integrity Protection
- Page Protection Layer

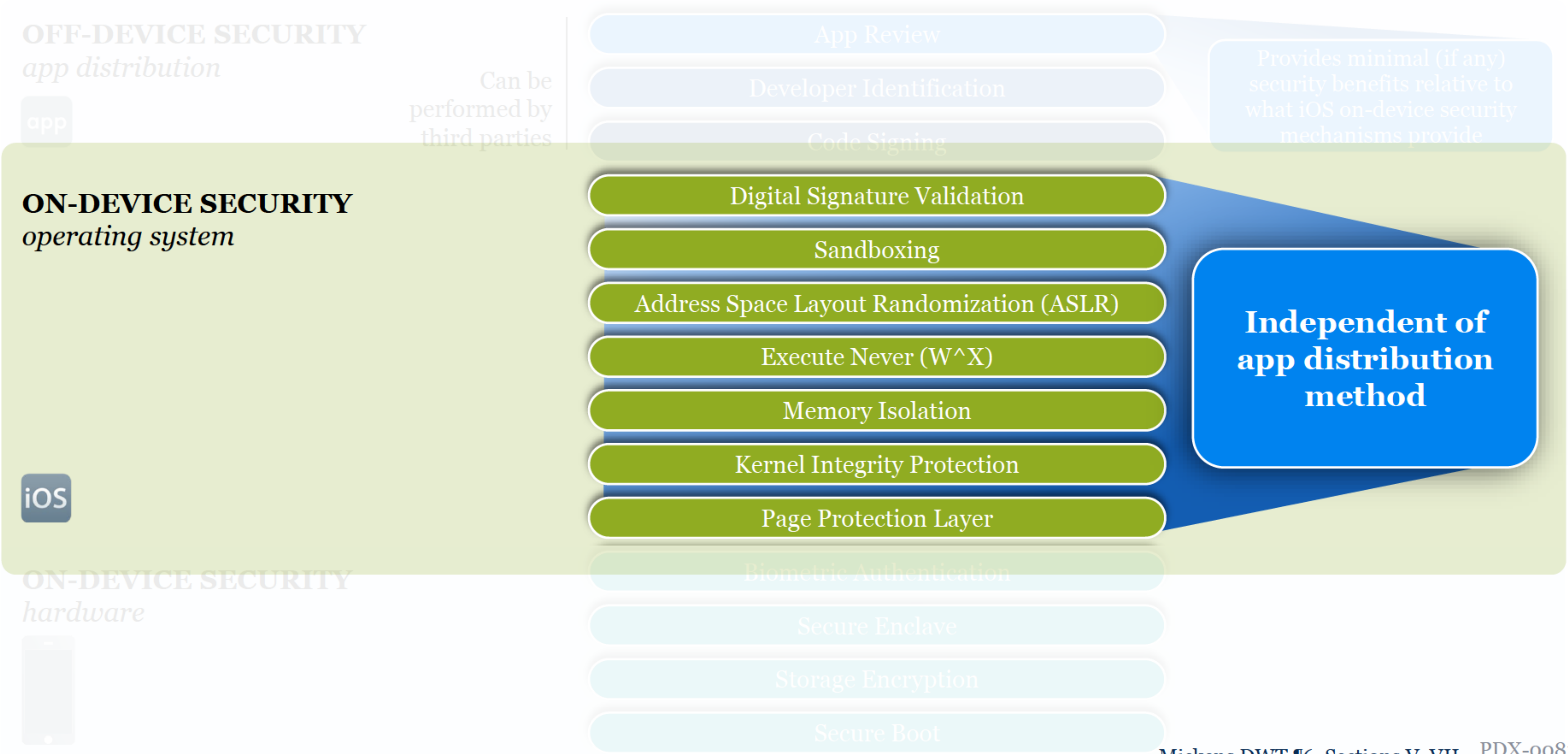
Examines code signatures, enabling various app distribution models

ON-DEVICE SECURITY
hardware

- Biometric Authentication
- Secure Enclave
- Storage Encryption
- Secure Boot

Mickens DWT Sections V, VII

On-Device Security: Operating System



OFF-DEVICE SECURITY
app distribution

Can be performed by third parties

- App Review
- Developer Identification
- Code Signing

Provides minimal (if any) security benefits relative to what iOS on-device security mechanisms provide

ON-DEVICE SECURITY
operating system

- Digital Signature Validation
- Sandboxing
- Address Space Layout Randomization (ASLR)
- Execute Never (W^X)
- Memory Isolation
- Kernel Integrity Protection
- Page Protection Layer

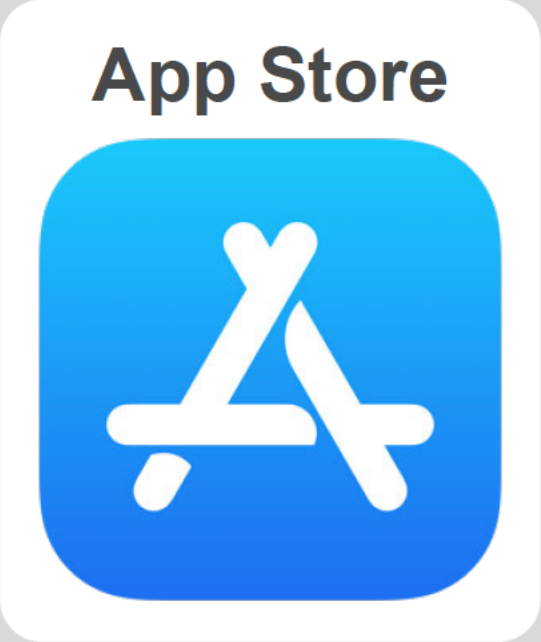
Independent of app distribution method

ON-DEVICE SECURITY
hardware

- Biometric Authentication
- Secure Enclave
- Storage Encryption
- Secure Boot

Mickens DWT ¶6, Sections V, VII

iOS: Models of App Distribution



iOS App Review: Security Properties

Security Properties

- Sandbox Compliance
- Exploit Resistance
- Malware Exclusion
- User Consent for Private Data
- Legal Compliance

iOS App Review: Security Properties

Security Properties	App Review	On-Device Security: Operating System
Sandbox Compliance	✓	Sandboxing ✓
Exploit Resistance	✓	ASLR KIP W^X PPL ✓
Malware Exclusion	✓	Anti-malware scanners ✓
User Consent for Private Data	weak, at best ⛓	System call monitoring ✓
Legal Compliance	**Difficult to ascertain by App Review or the OS**	

iOS: Models of App Distribution

App Store

Apple Developer Enterprise Program

Internal Apple Testing Distribution

iOS App Distribution Models: Security Features

	ON-DEVICE SECURITY *operating system*	**OFF-DEVICE SECURITY** *app distribution*		
	Digital Signature Validation Sandboxing Address Space Layout Randomization (ASLR) Execute Never (W^X) Memory Isolation Kernel Integrity Protection Page Protection Layer	App Review	Developer Identification	Code Signing
App Store	✓	✓	✓	✓
Apple Developer Enterprise Program	✓	✗	Partially	Not by Apple
Internal Apple Testing Distribution	✓	✗	✓	✗

macOS Operating System

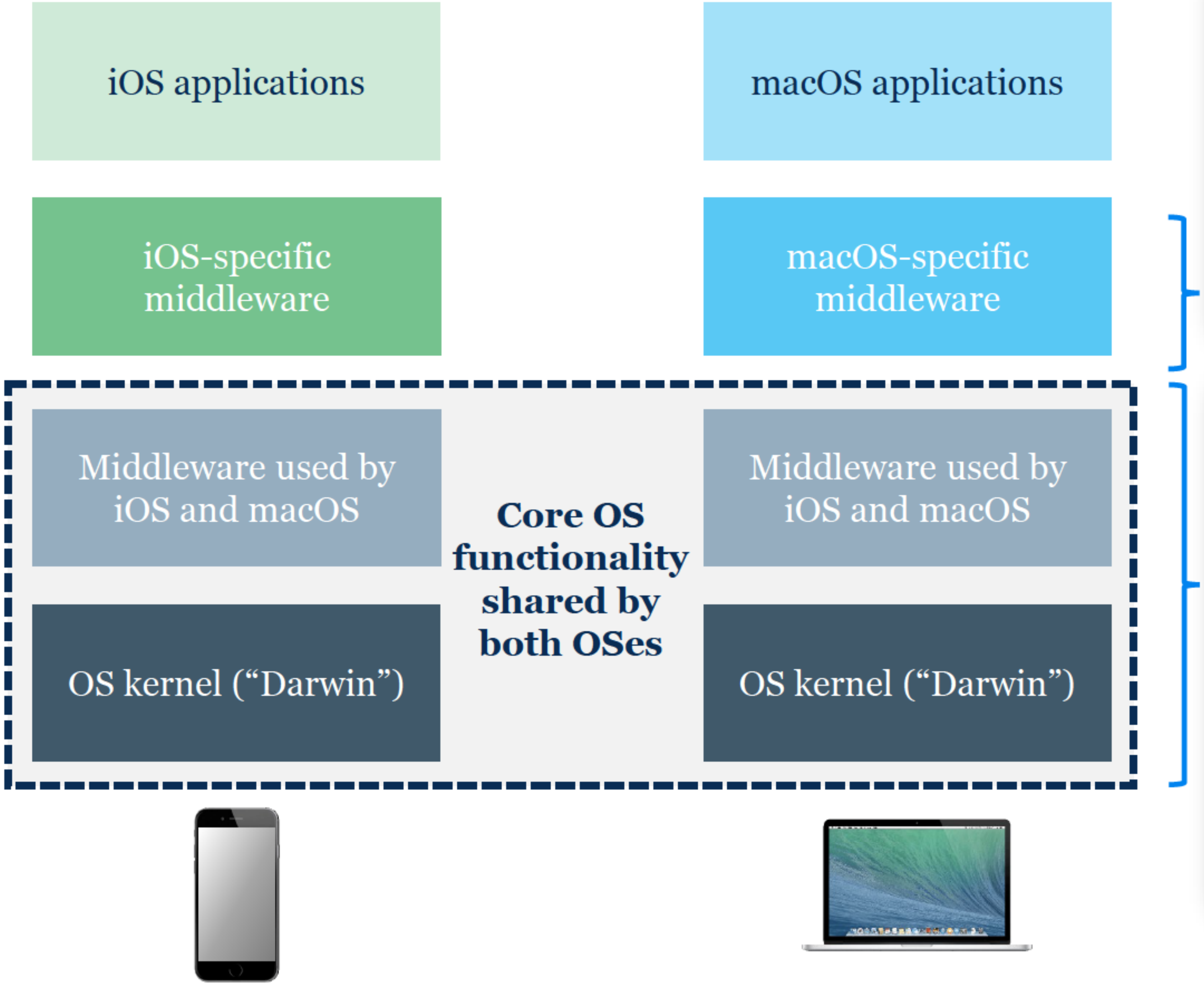
macOS: Models of App Distribution

Mac App Store

Third Party Distribution
(Notarization)

Third Party Distribution
(unreviewed + unnotarized)

iOS vs. macOS Software Layers



<u>Responsible for</u>:

- Providing higher-level “friendlier” mechanisms for users and developers to communicate with hardware
- Customizing core OS-level security features

<u>Responsible for:</u>

- Implementing the lowest-level (*i.e.*, the most basic) management tasks like resource allocation and application scheduling
- **Enforcing core OS-level security features** (e.g., ASLR, W^X, etc.) or providing the basic framework for those features (e.g., sandboxing)

How is Security Enforced on iOS and macOS?

Off-Device Security: App Distribution

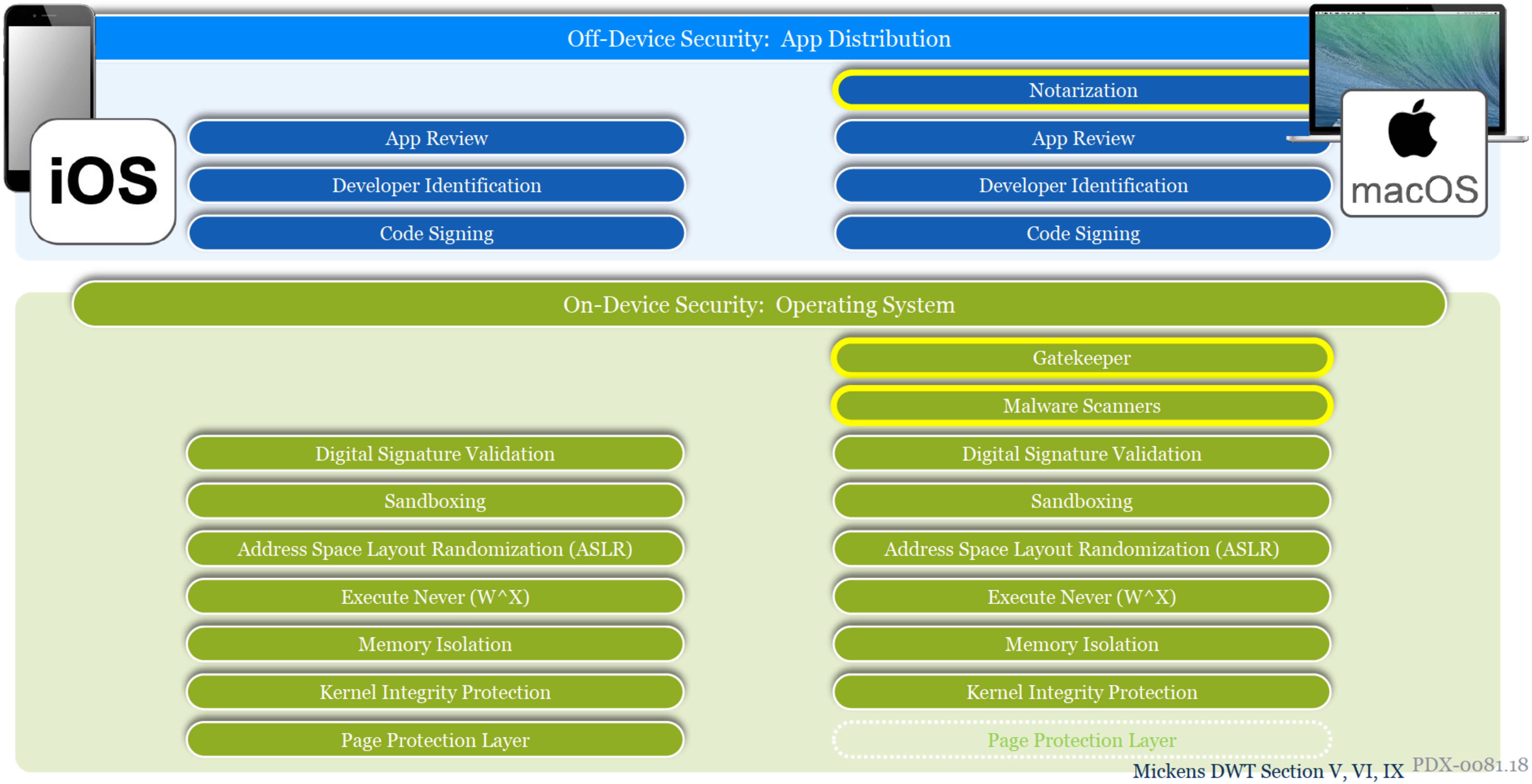
iOS	macOS
App Review	App Review
Developer Identification	Developer Identification
Code Signing	Code Signing

On-Device Security: Operating System

iOS	macOS
Digital Signature Validation	Digital Signature Validation
Sandboxing	Sandboxing
Address Space Layout Randomization (ASLR)	Address Space Layout Randomization (ASLR)
Execute Never (W^X)	Execute Never (W^X)
Memory Isolation	Memory Isolation
Kernel Integrity Protection	Kernel Integrity Protection
Page Protection Layer	Page Protection Layer

Mickens DWT Section V, VI

How is Security Enforced on iOS and macOS?



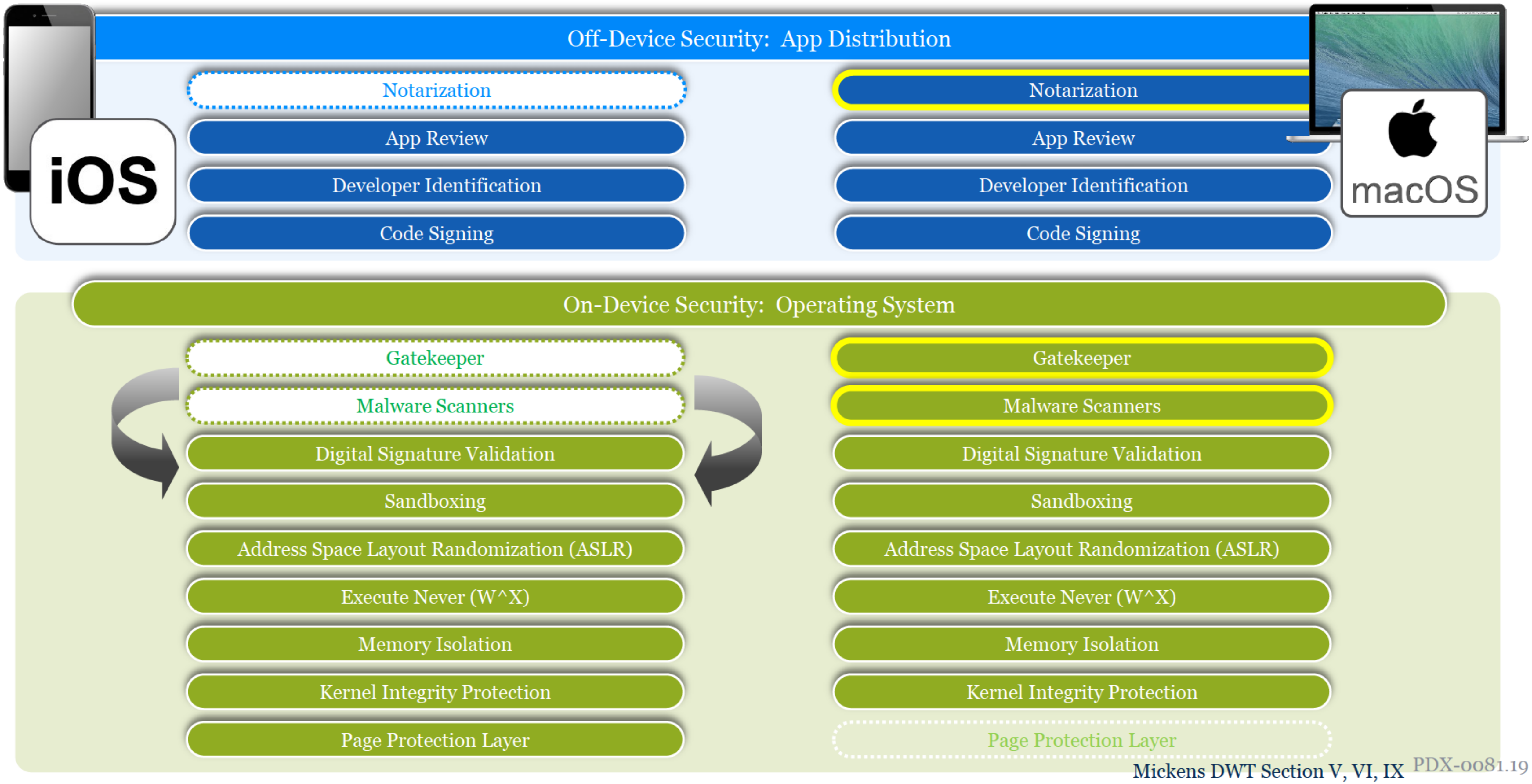
Off-Device Security: App Distribution

iOS	macOS
	Notarization
App Review	App Review
Developer Identification	Developer Identification
Code Signing	Code Signing

On-Device Security: Operating System

iOS	macOS
	Gatekeeper
	Malware Scanners
Digital Signature Validation	Digital Signature Validation
Sandboxing	Sandboxing
Address Space Layout Randomization (ASLR)	Address Space Layout Randomization (ASLR)
Execute Never (W^X)	Execute Never (W^X)
Memory Isolation	Memory Isolation
Kernel Integrity Protection	Kernel Integrity Protection
Page Protection Layer	Page Protection Layer

How is Security Enforced on iOS and macOS?



Off-Device Security: App Distribution

iOS	macOS
Notarization	Notarization
App Review	App Review
Developer Identification	Developer Identification
Code Signing	Code Signing

On-Device Security: Operating System

iOS	macOS
Gatekeeper	Gatekeeper
Malware Scanners	Malware Scanners
Digital Signature Validation	Digital Signature Validation
Sandboxing	Sandboxing
Address Space Layout Randomization (ASLR)	Address Space Layout Randomization (ASLR)
Execute Never (W^X)	Execute Never (W^X)
Memory Isolation	Memory Isolation
Kernel Integrity Protection	Kernel Integrity Protection
Page Protection Layer	Page Protection Layer

App Distribution: Design Implications

		On-Device OS Security Features	Apps Reviewed by Apple	Apps Signed By:
	**App Store**	**Yes**	**Yes**	**Apple**
	Developer Enterprise	**Yes**	**No**	**Enterprise developer**
	Internal Apple Testing Distribution	**Yes**	**No**	**Nobody**
	**Mac Store**	**Yes**	**Yes**	**Apple**
	Notarized	**Yes**	**Yes (malware scan only)**	**Third-party developer**
	Unsigned Third-Party	**Yes**	**No**	**Third-party developer or nobody**